Integrierte IT-Service-Management-Lösungen anhand von Fallstudien

„Fallbeispiele 2“

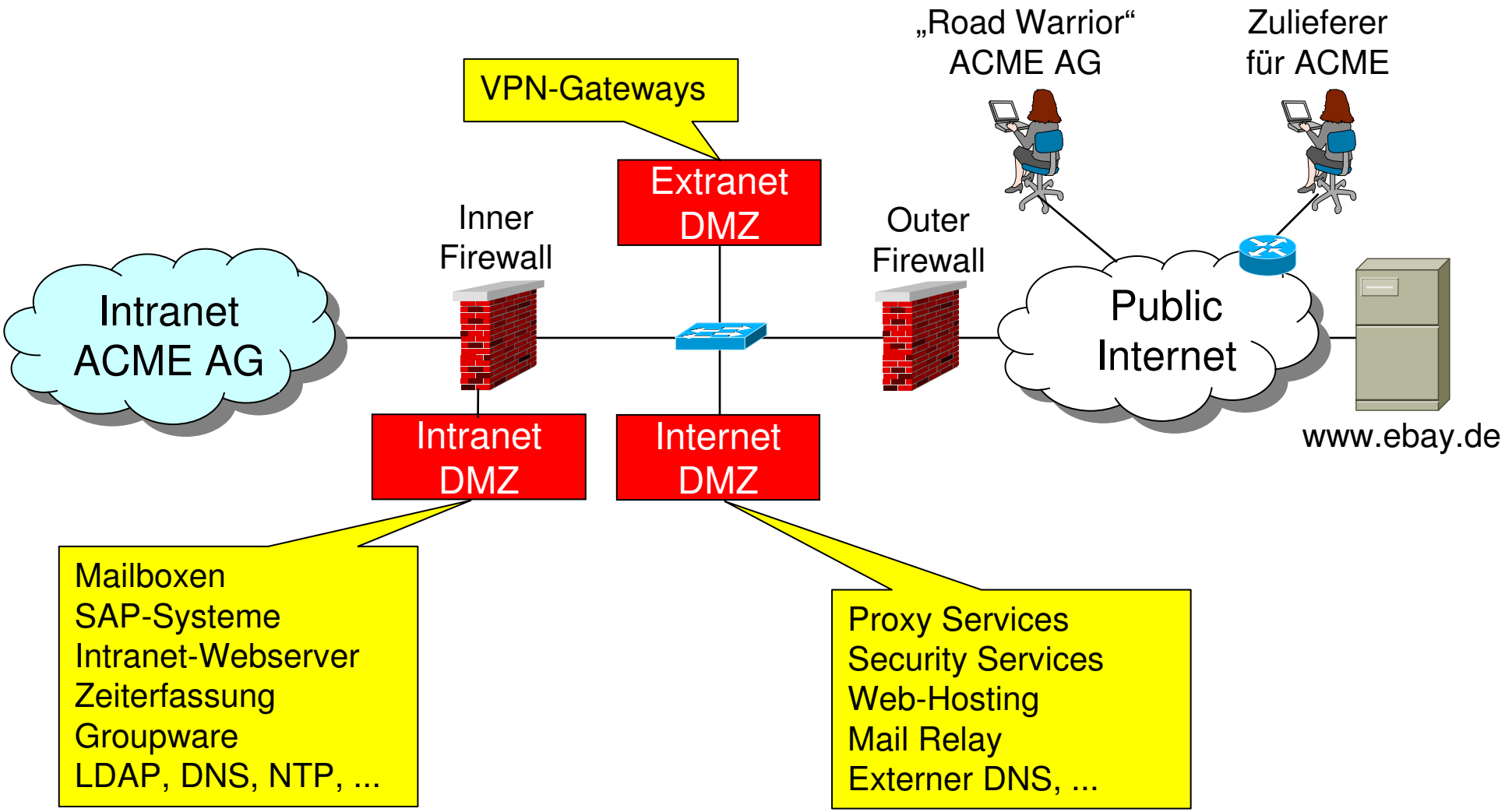
Spezielle Anforderungen, Realisierung, RZ-Infrastrukturen, Operatives Management

Dr. Michael Nerb et al.,
Prof. Dr. Heinz-Gerd Hegering

SoSe 2008

Wiederholung – Design der zentralen Dienste

Mögliche Variante der Internet-Anbindung und DMZ



Design des DNS
Anforderungen und Entscheidungsfindung

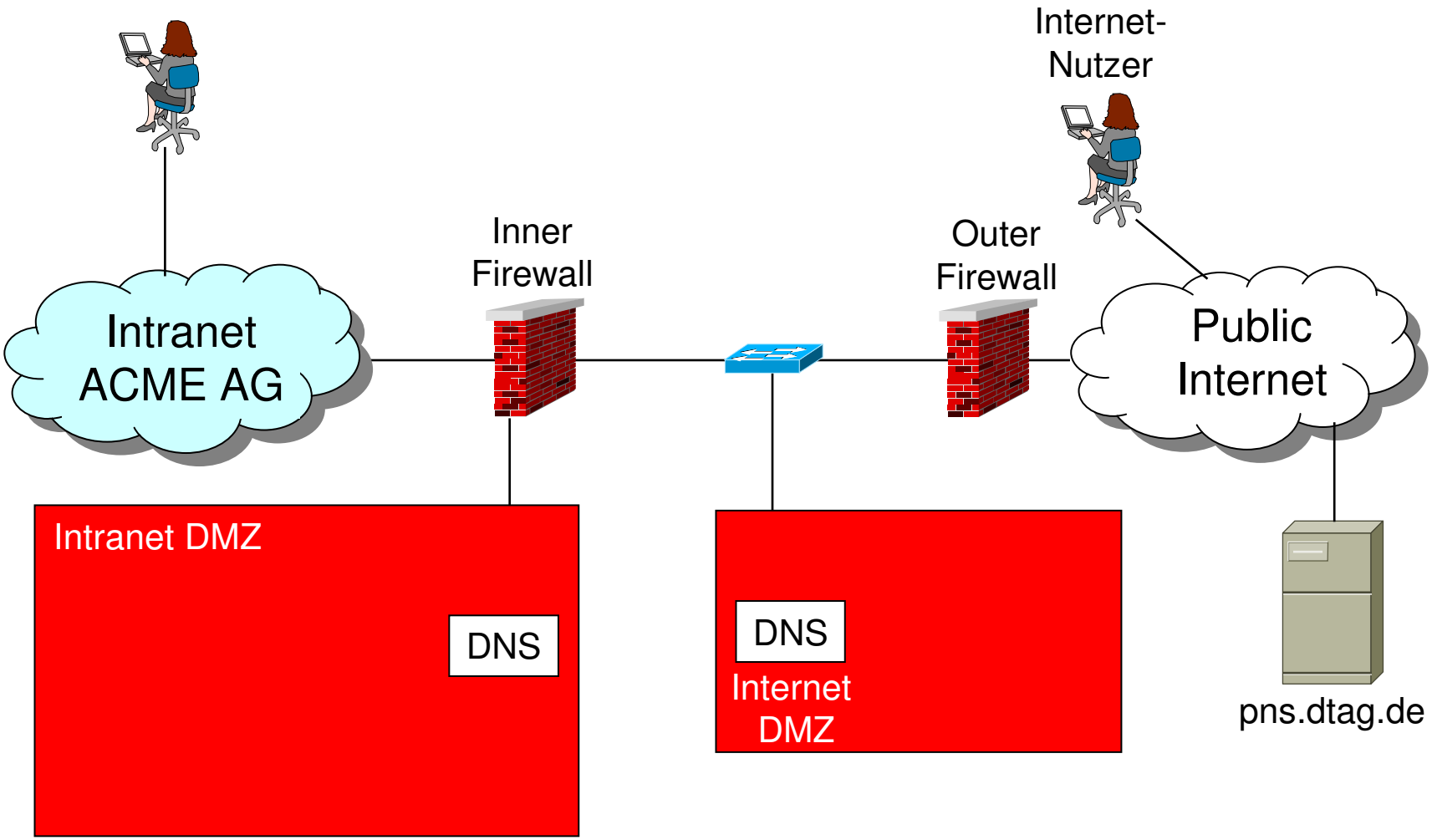
- Domain Name System (DNS) soll unter der Hoheit der ACME AG liegen
- DNS dient der internen und externen Namensauflösung, d.h.:
  - Abbildung interner Namen, z.B. intranet.acme.intern (nicht im Internet sichtbar)
  - Abbildung externer Namen z.B. www.acme.de, vpn.acme.de, mail.acme.de (aber auch .com, .net oder .org Top-Level-Domains)
  - Auflösen von Namen aus dem Internet (z.B. www.cisco.com)

- Abstützen auf einen Secondary Nameserver im Internet (z.B. pns.dtag.de)
- Zusätzliche Sicherung des DNS durch „Verstecken“ des ACME DNS hinter dem Secondary DNS („Hidden Primary“)

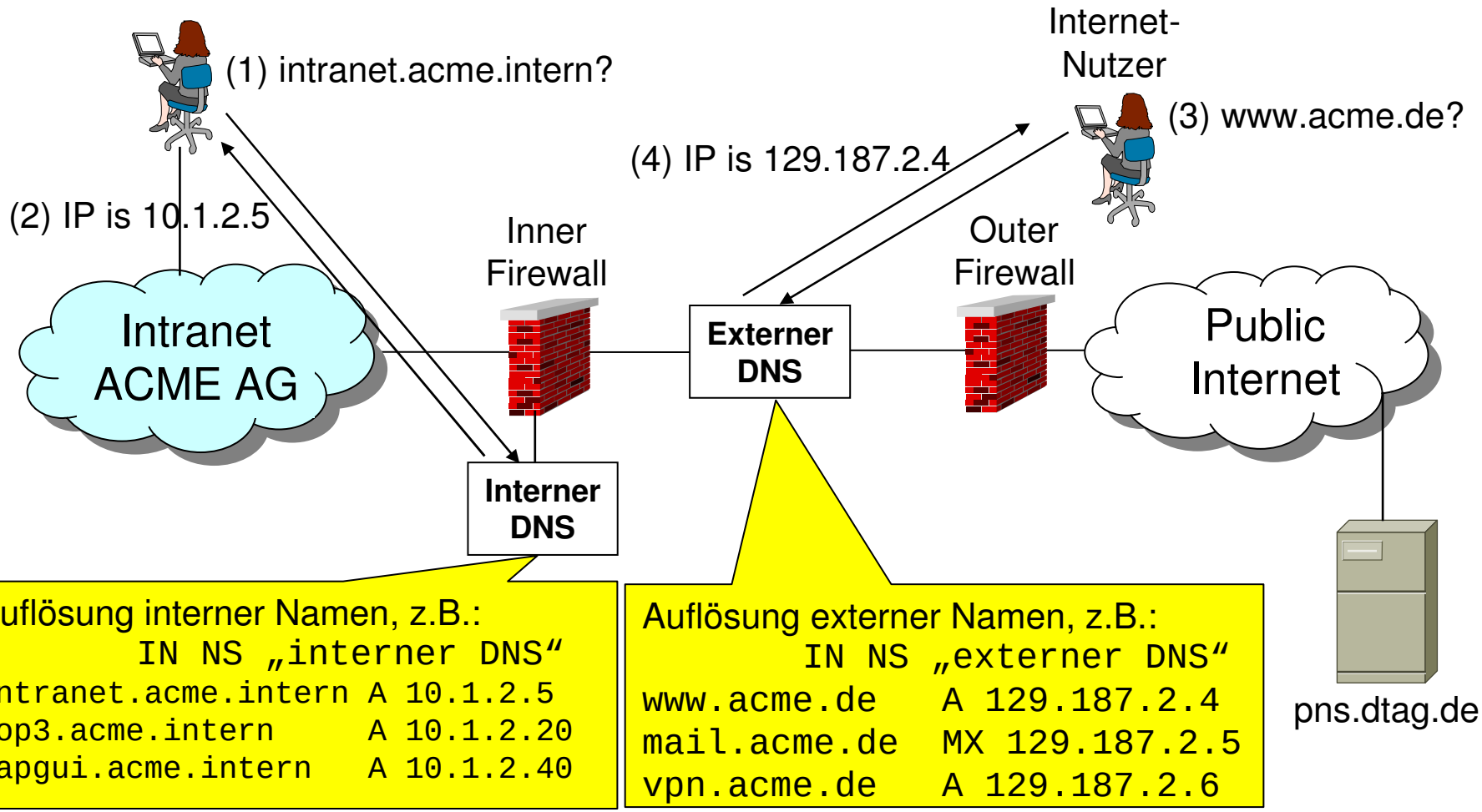
- Entscheidungsfindung:
  - Keine wirkliche Alternative zur Open Source Lösung „BIND“

Realisierung des DNS

Benötigte Systeme

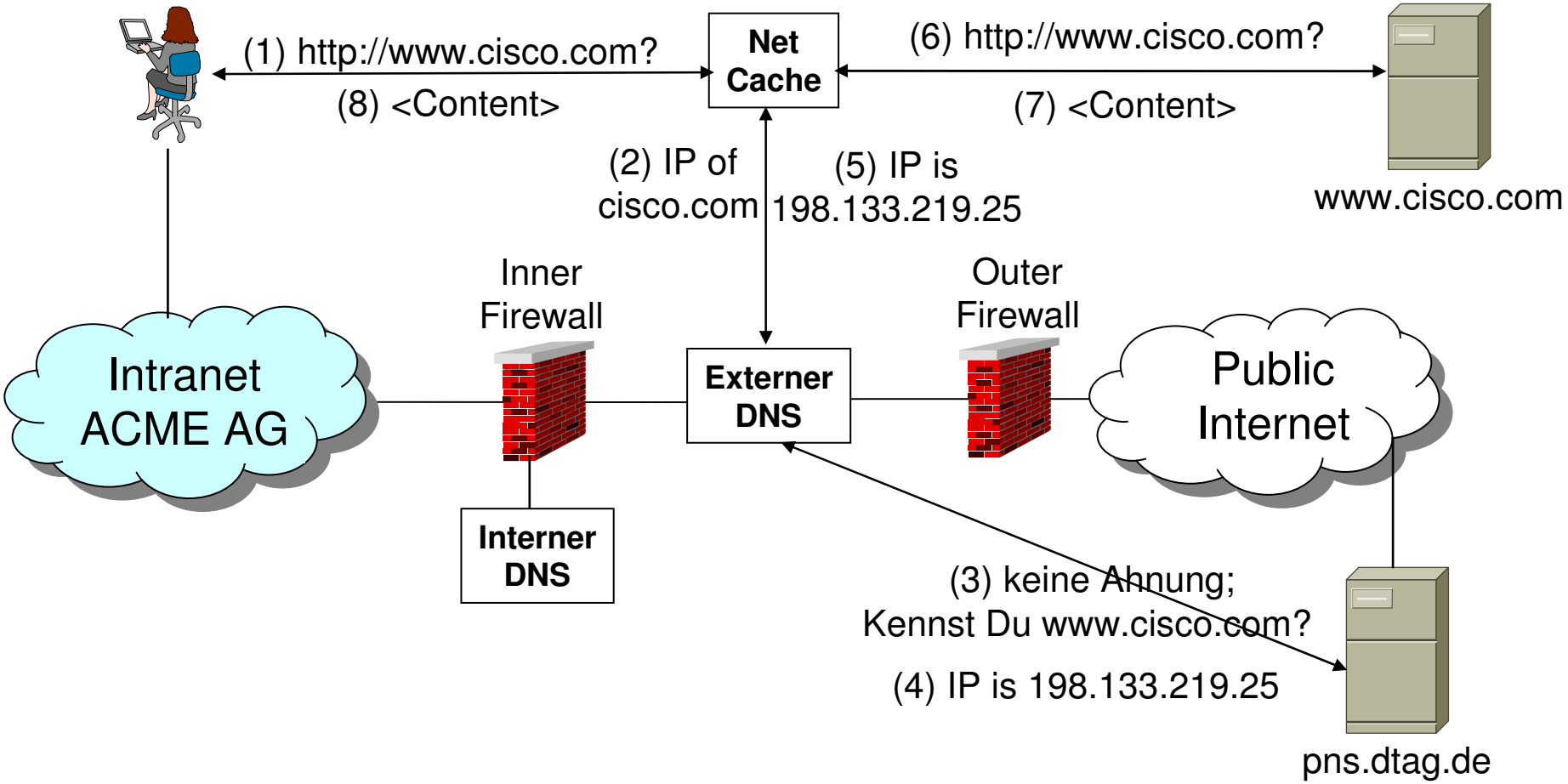


Realisierung des DNS
Kommunikationsflüsse und Nutzung der Dienste (1)



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

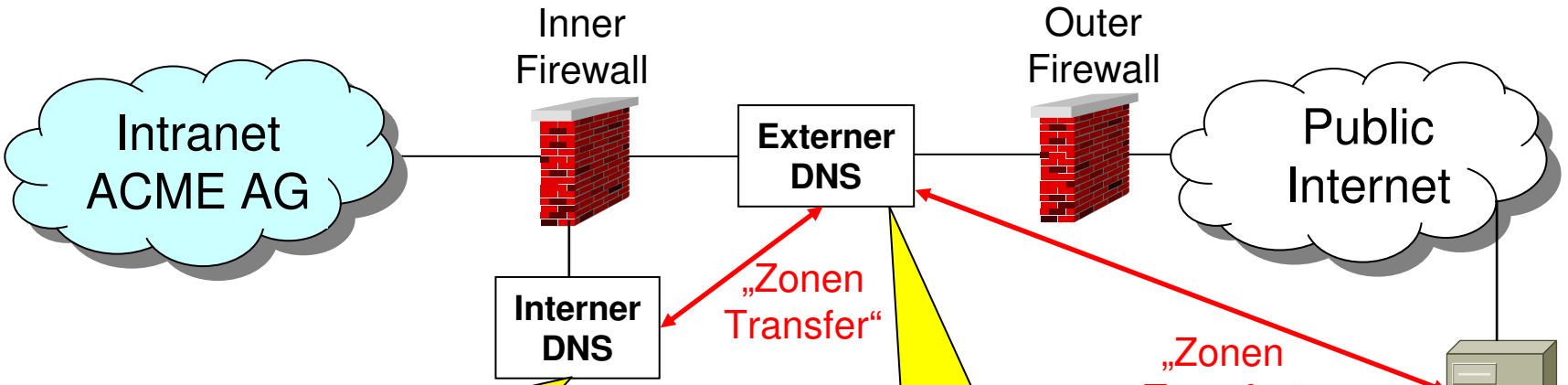
Realisierung des DNS
Kommunikationsflüsse und Nutzung der Dienste (2)



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Realisierung des DNS

Advanced Features: Zonentransfer (Exkurs)



„Master“ für interne Namen, z.B.:

```
        IN NS „interner DNS“
Intranet.acme.intern A 10.1.2.5
pop3.acme.intern     A 10.1.2.20
Sapgui.acme.intern   A 10.1.2.40
```

„Master“ für externe Namen, z.B.:

```
        IN NS „externer DNS“
www.acme.de   A 129.187.2.4
mail.acme.de  MX 129.187.2.5
vpn.acme.de   A 129.187.2.6
```

„Slave“ für externe Namen, z.B.:

```
        IN NS „externer DNS“
www.acme.de   A 129.187.2.4
mail.acme.de  MX 129.187.2.5
vpn.acme.de   A 129.187.2.6
```

(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Design des Mail-Dienstes (Relay und Mailboxen)
Anforderungen

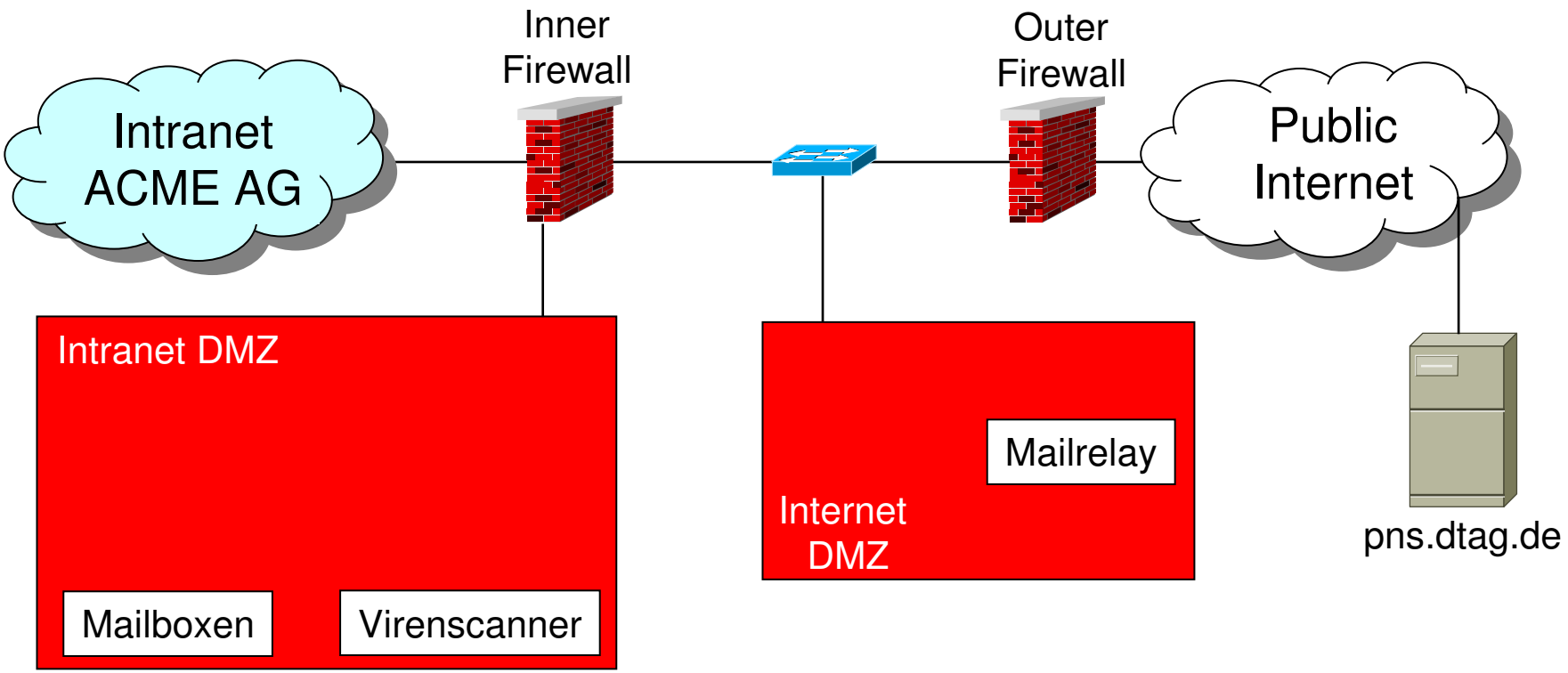
- „Mail-Relay“:
  - Entgegennahme von Mails für ACME Mitarbeiter:
    - Anti-Virus (Schutz vor Mailviren)
    - Anti-SPAM (Schutz vor unerwünschten Mails)
    - Anti-Relaying (Schutz vor Missbrauch des Mail-Relays)
  - Versenden von Mails von ACME Mitarbeitern ins Internet:
    - Anti-Virus
    - Anti-Spoofing (Schutz vor Missbrauch von Usernamen)
  - Zwischenspeichern von eingehenden/ausgehenden Mails für eine gewisse Zeit (z.B. falls Mailboxen/Mail-Relays) „voll“ sind
- „Mail-Boxen“:
  - Speichern von Mails in Mailboxen der (ca. 5.000) User
  - Zugriff über POP3 und/oder IMAP4, Quota: 100 Mbyte/User
  - Virenscanning (von lokaler ausgelieferter Mail)
  - Sicherung und Backup des Mailbox-Servers
    - Bei 5.000 User und 100 Mbyte Quota: 500 Gbyte!

Design des Mail-Dienstes (Relay und Mailboxen)
Entscheidungsfindung

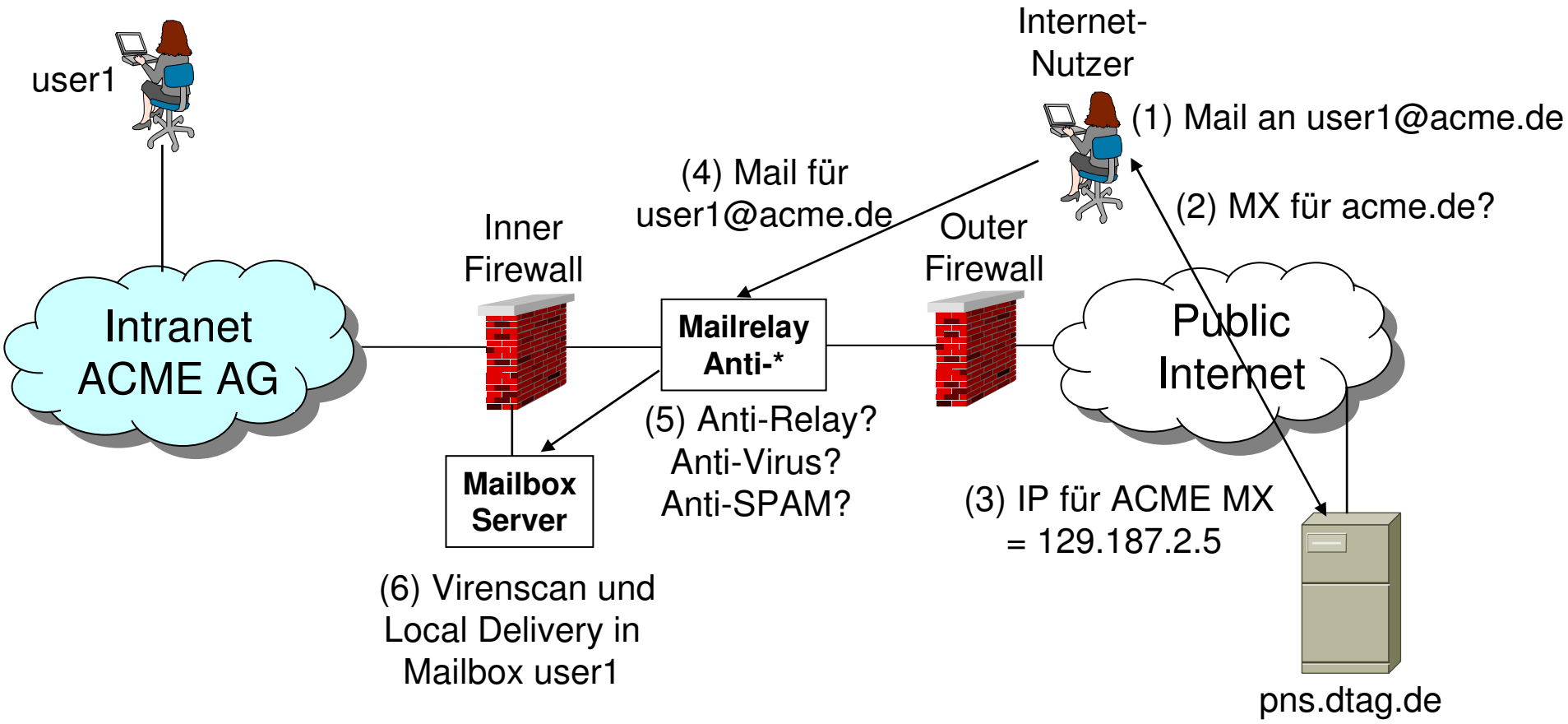
- Produkte:
  - Mail-Relays: Sendmail und/oder Postfix
  - Mailbox-Server: Cyrus-IMAPD, POP3D, SuSE Open Exchange Server, Microsoft Exchange Server
  - Webwasher (SMTP-Relay mit umfangreichen Anti-* Funktionen)
  - Novell Netmail, Diverse Virenscanner für „Batch“ Scanning
- Einige Entscheidungskriterien:
  - Kommerzielle Produkte vs. Open Source
  - Unterstützung von Groupware-Funktionalitäten und Microsoft Produkten
  - Integration der Anti-* Funktionen
  - Wartung, Support und Flexibilität
- Entscheidung:
  - Webwasher mit Anti-* Funktionen als Mail-Relay
  - Cyrus-IMAPD, POP3D für Mailboxen

Realisierung Mail-Dienst (Relay und Mailboxen)

Benötigte Systeme

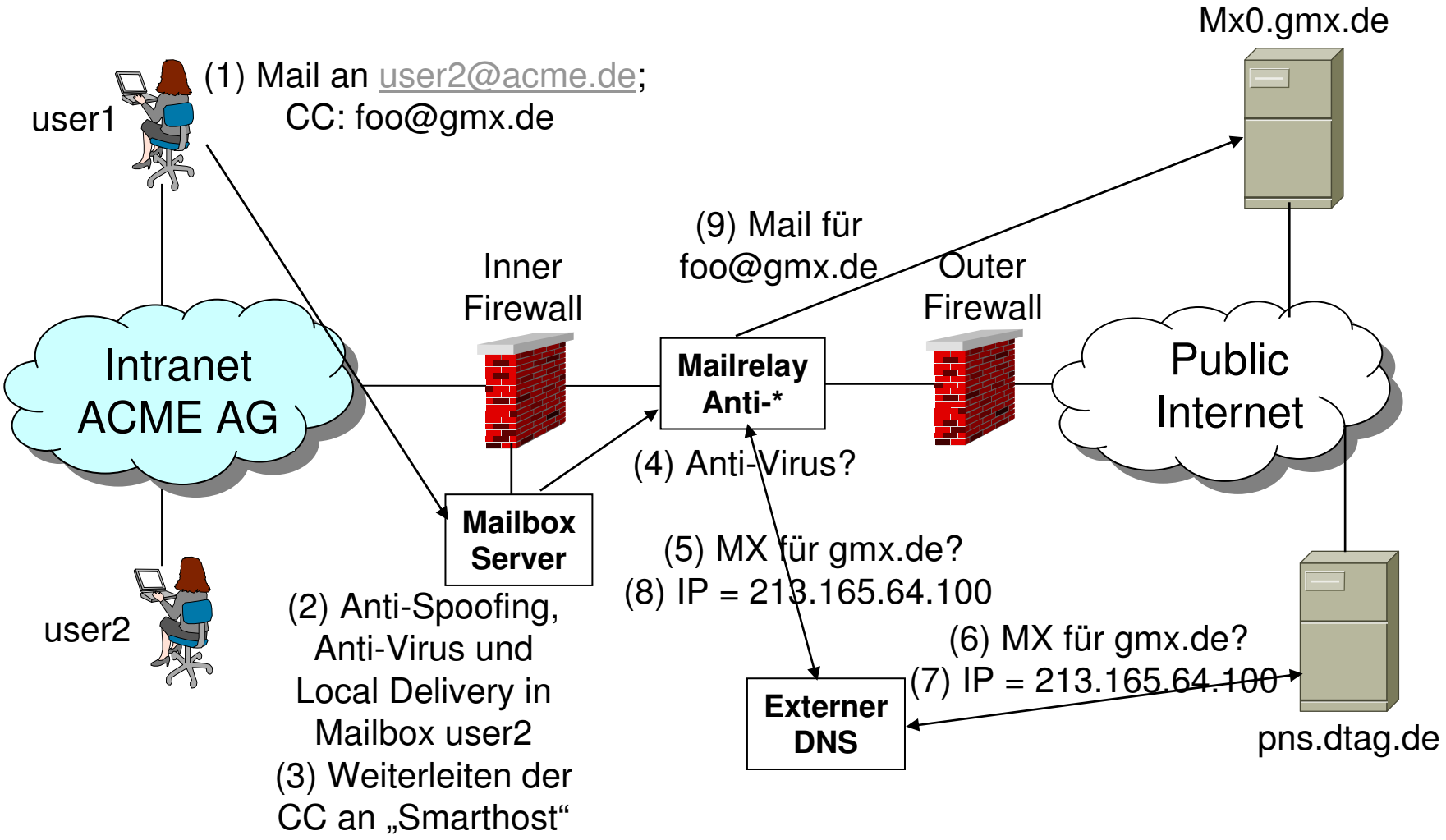


Realisierung des Mail-Relays (eingehende Mail)
Kommunikationsflüsse und Nutzung der Dienste



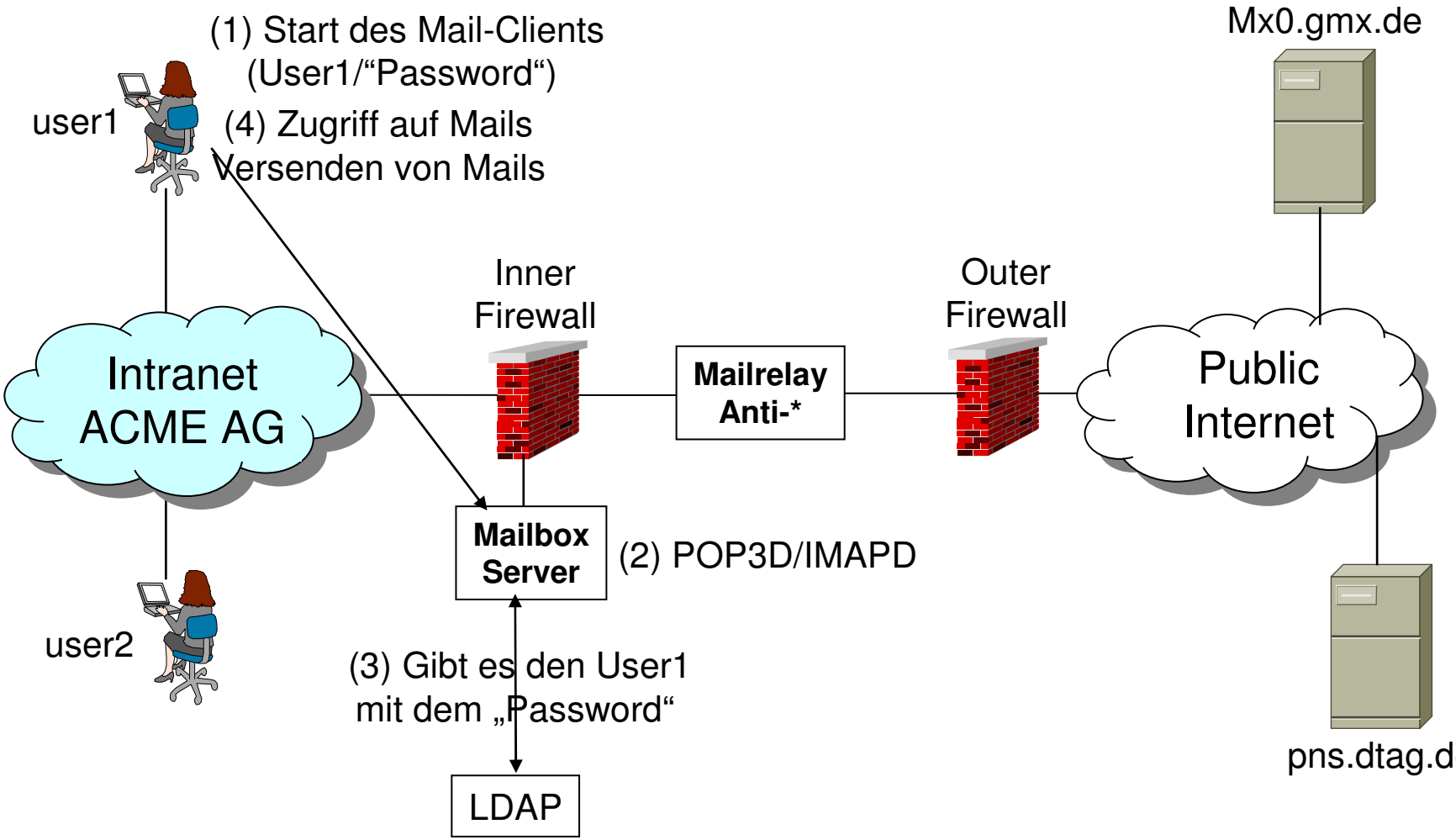
(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Realisierung des Mail-Relays (ausgehende Mail)
Kommunikationsflüsse und Nutzung der Dienste



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

Realisierung der Mail-Boxen
Kommunikationsflüsse und Nutzung der Dienste



(Vereinfachte Darstellung! Alle Kommunikationsflüsse gehen natürlich durch die Firewalls von und zu den entsprechenden DMZ!)

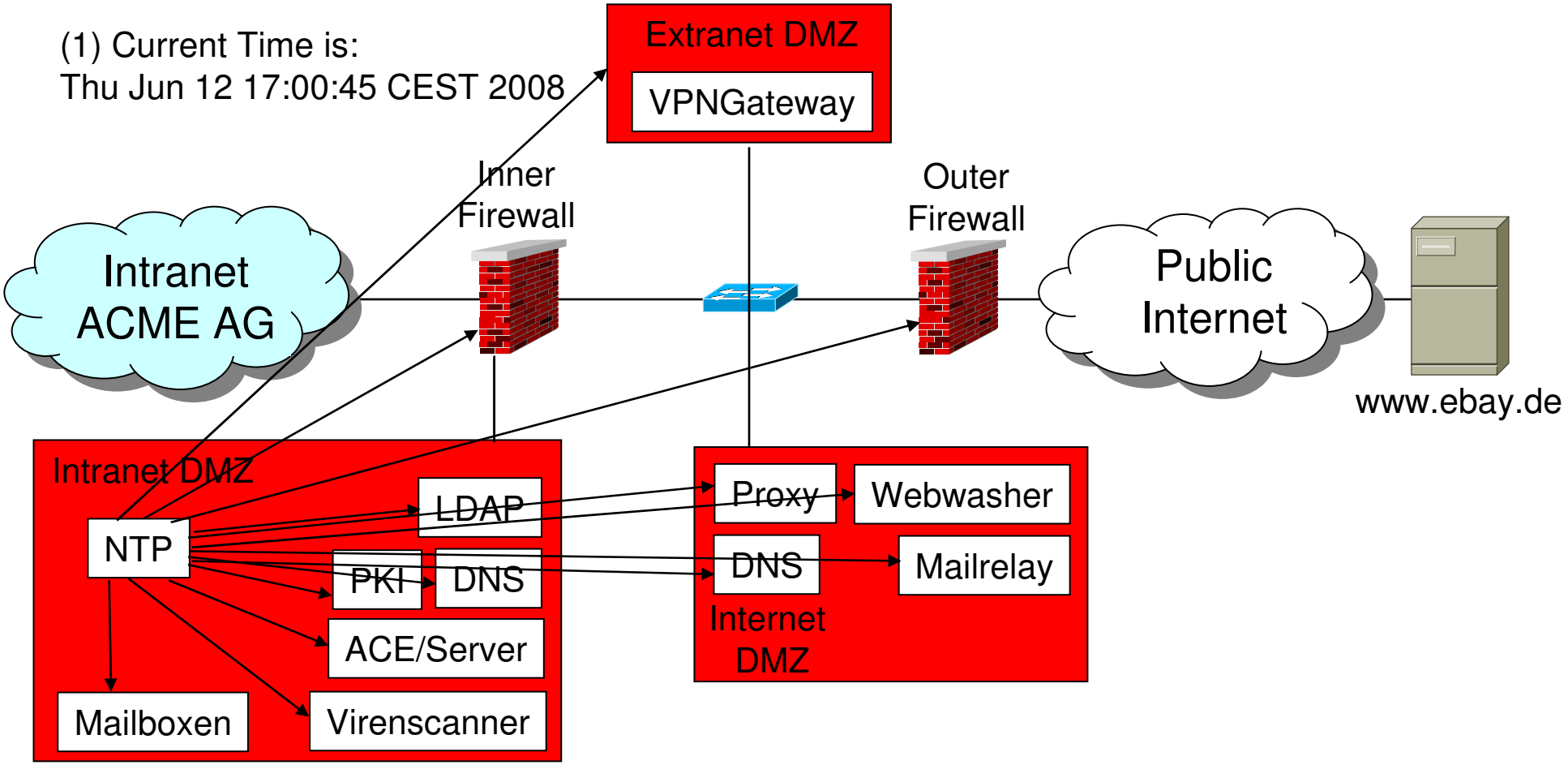
Design des NTP Services
Anforderungen und Entscheidungsfindung

- Alle Server sollen auf „die gleiche Zeit“ synchronisiert werden
- Zeitsynchronität soll auf einer Referenz-Uhrzeit basieren, z.B.:
  - DCF-77 (Sender der Physikalisch-Technischen Bundesanstalt)
  - GPS (Global Positioning System)
- Produkte:
  - Open Source: NTPD (Software zur Verteilung der Zeitinformation)
  - DCF-77 Empfänger: Hirschmann, Netgear, (oder bei Conrad ;-)
  - Oder: Nutzung einer Zeitquelle aus dem Internet
- Entscheidungskriterien:
  - Empfang im Rechenzentrum (bzw. wo muss der Empfänger im Rechenzentrum positionieren)

- Entscheidung für ACME AG:
  - DCF-77 Empfänger und NTPD

Realisierung des NTP Services

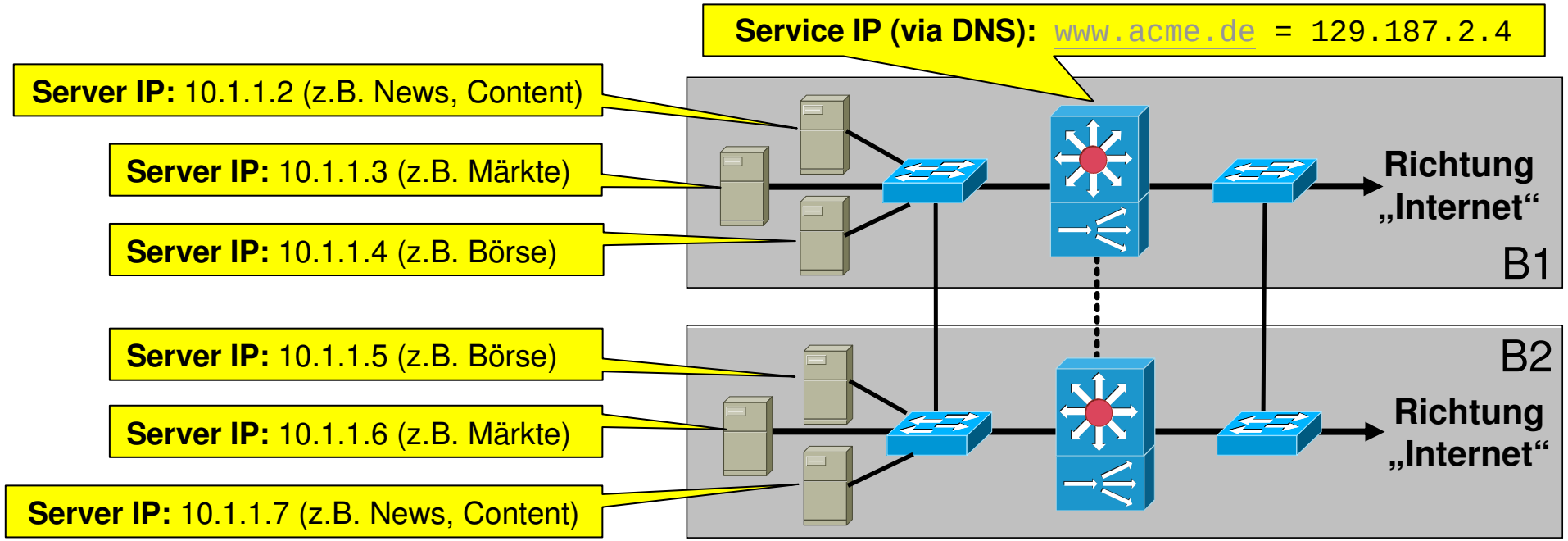
Benötigte Systeme und Kommunikationsflüsse



Design des Web-Hostings
Anforderungen

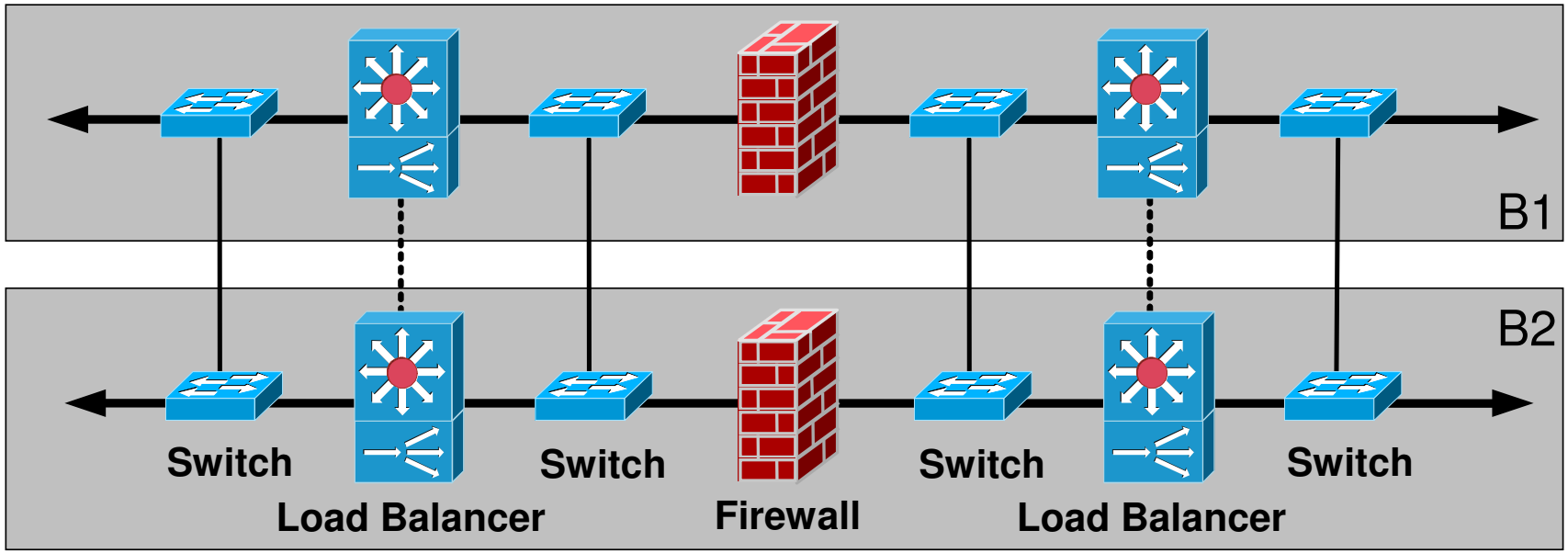
- Internetpräsenz für www.acme.de:
  - Portal für eine Tageszeitung
  - Redaktioneller Content (News, Börse, Weltgeschehen usw.)
  - Marktplätze (Job-, Immo-, KfZ-, Partnerbörse usw.)
  - Diskussionsforen
- Betriebliche, organisatorische und technische Anforderungen:
  - Rechenzentrumsinfrastruktur, Internet-Konnektivität
  - Hochverfügbarkeit und Redundanz
  - Performanz, Flexibilität und Skalierbarkeit
- Bereitstellung von entsprechenden Inhalten (Content):
  - Statische und dynamische Inhalte
  - Möglichkeiten für Kommentare, Postings, Newsletter usw.

Design der Hochverfügbarkeit
Server Load Balancing für „www.acme.de“



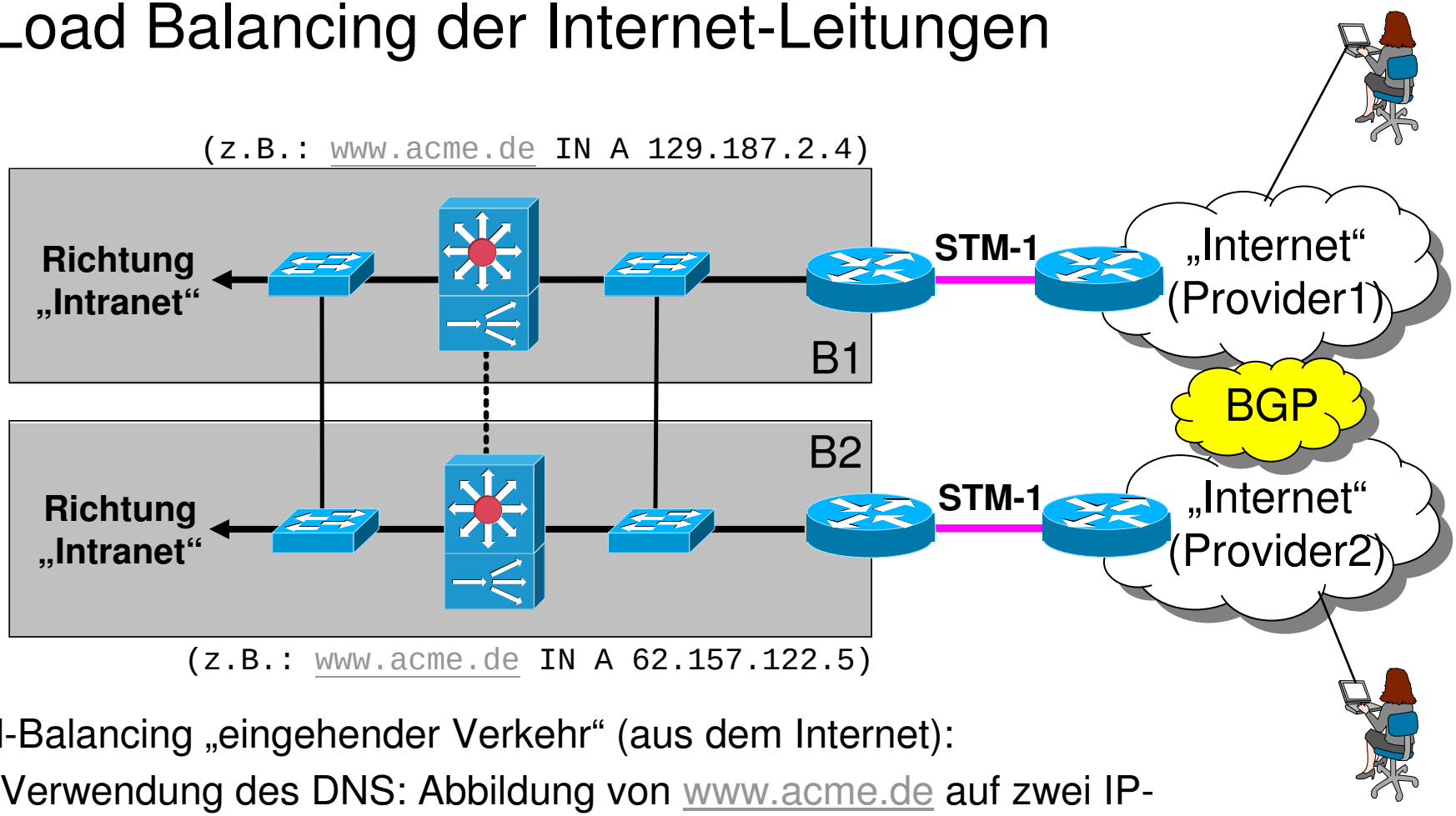
- Funktionen der Load-Balancer: u.a. Lastverteilung, Redundanz, Session-Persistenz, Network Address Translation (NAT)
- Ausprägungen:
  - Server Load Balancer, Layer 4-7 Switch
  - Nur bedingt: Application Proxy, Port Forwarder
- Unterscheidungskriterien (u.a.):
  - Implementierung in HW/SW, OSI-Schicht, Unterstützte Protokolle
- Hersteller: z.B. F5 Networks, Radware, Alteon, ...

Design der Hochverfügbarkeit
Redundanz über zwei Brandabschnitte (B1/B2)



- Betriebsmodus „Active/Active“:
  - Beide Systeme bedienen Requests (Load-Balancing)
  - Systeme überwachen sich gegenseitig auf Ausfall
- Betriebsmodus „Active/Standby“:
  - „Aktives System“ bedient alle Requests
  - „Standby System“ übernimmt bei Ausfall (Fail-Over)

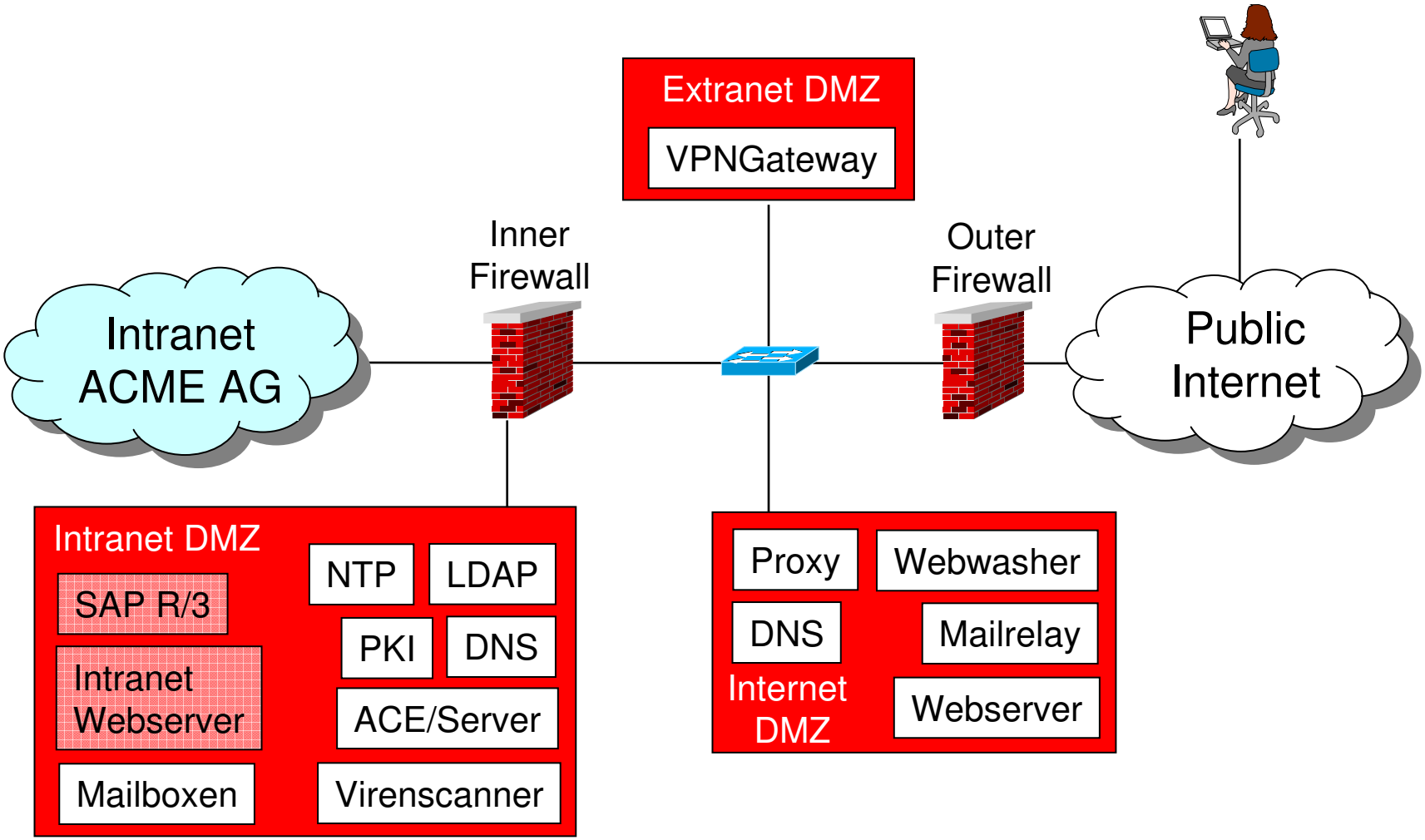
Design der Hochverfügbarkeit
Load Balancing der Internet-Leitungen



- Load-Balancing „eingehender Verkehr“ (aus dem Internet):
  - Verwendung des DNS: Abbildung von www.acme.de auf zwei IP-Adressen (je eine aus dem IP-Adressbereich Provider1 und Provider 2)
- Load-Balancing „ausgehender Verkehr“ (ins Internet):
  - Entweder: „Gleicher Weg zurück“ (LB hält „Session-Information“)
  - Andernfalls: Load-Balancer kann „frei“ auf beide Leitungen verteilen

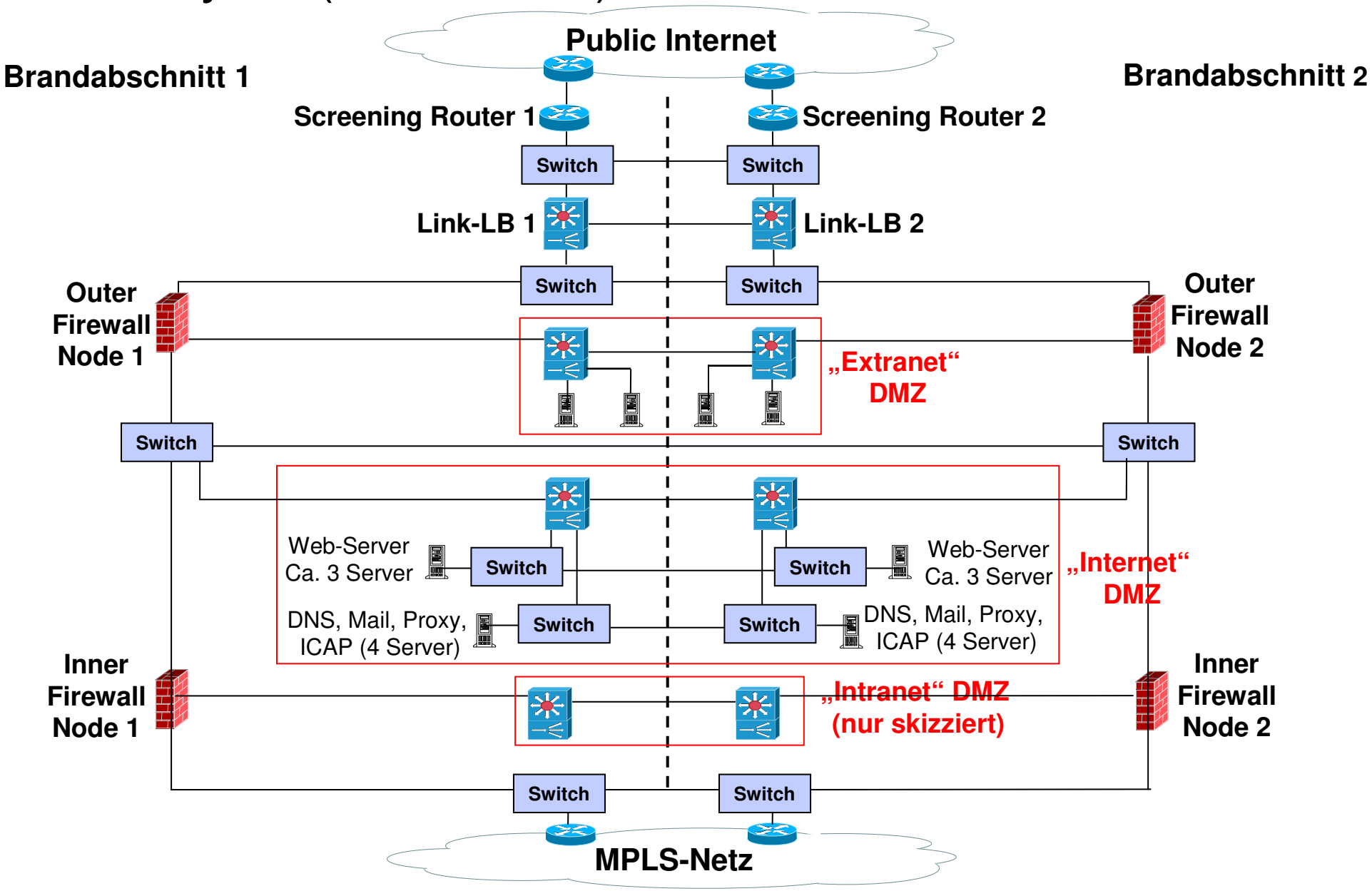
Design der zentralen Dienste

Zusammenfassung: „Service View“ auf alle Dienste



Realisierung der Services

Layout (vereinfacht), „Server View“



Realisierung der Services
Rechenzentrumsinfrastruktur und zentrale Dienste

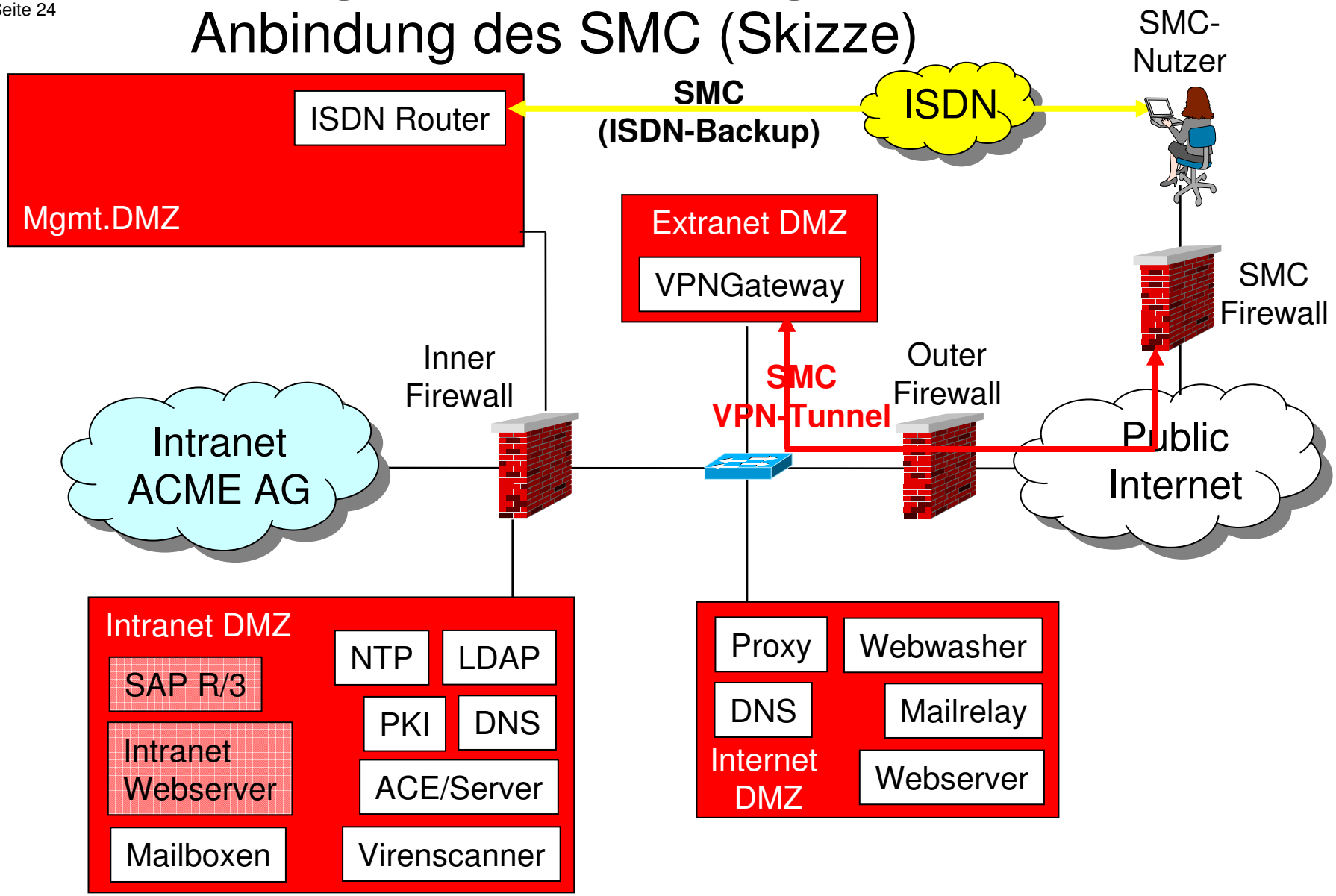
- Infrastruktur:
  - Strom, Diesel, USV, Klima
  - Brandschutz, Zugangskontrolle, Gebäudeleittechnik
- Zentrale Dienste:
  - „Rackspace“, LAN-Connectivity, Glasfasern
  - Internet-Connectivity, Remote Access (z.B. über ISDN-Einwahl)
  - Backup und Filesysteme, z.B.:
    - Network Attached Storage (NAS)
    - Storage Area Networks (SAN)
  - Archivierung (Tape Libraries, Bandroboter, Safes)
- Personal vor Ort:
  - „Remote Hands“ für Power Cycling, Reboot o.ä.
  - Bedienung von „Konsolenswitches“ (Monitor, Maus, Tastatur-Umschalter)

Management der Lösung
Randbedingungen und Anforderungen

- Server (Rechenzentrum) und betriebliches Management sind örtlich getrennt
- Alle Services sind hochverfügbar:
  - Mindestens zwei Server pro Service
  - Gegenseitige Überwachung mit Fail-Over und ggf. Load-Balancing
- Zu jedem Server gibt es mindestens 2 Wege:
  - Auf dem Weg vom „Betriebszentrum“ (SMC) zum Rechenzentrum
  - Innerhalb des Rechenzentrums
- Anbindung der Server zum Backup (SAN/NAS) erfolgt über separates Netz
- Server und Services werden geeignet überwacht:
  - Mindestens: Server: SNMP, Services: Nagios
  - Zusätzlich: Web-Based Management über Browser-GUI‘s für Server und Services (je nach Möglichkeiten der einzelnen Produkte)
- Sicherung von relevanten Dateien von den Servern, z.B.:
  - Konfigurationsdateien: Für eine schnelle Wiederherstellung
  - Logdateien: Für eine Aufbereitung, z.B. der Dienstnutzung durch User

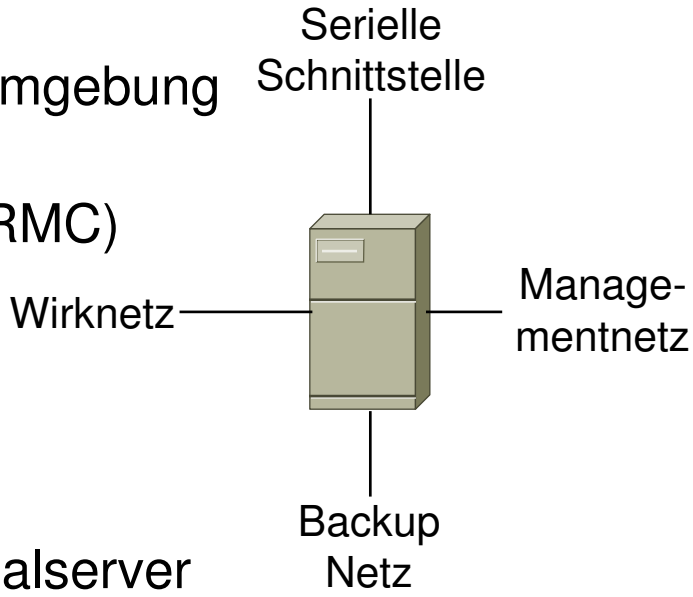
Management der Lösung

Anbindung des SMC (Skizze)

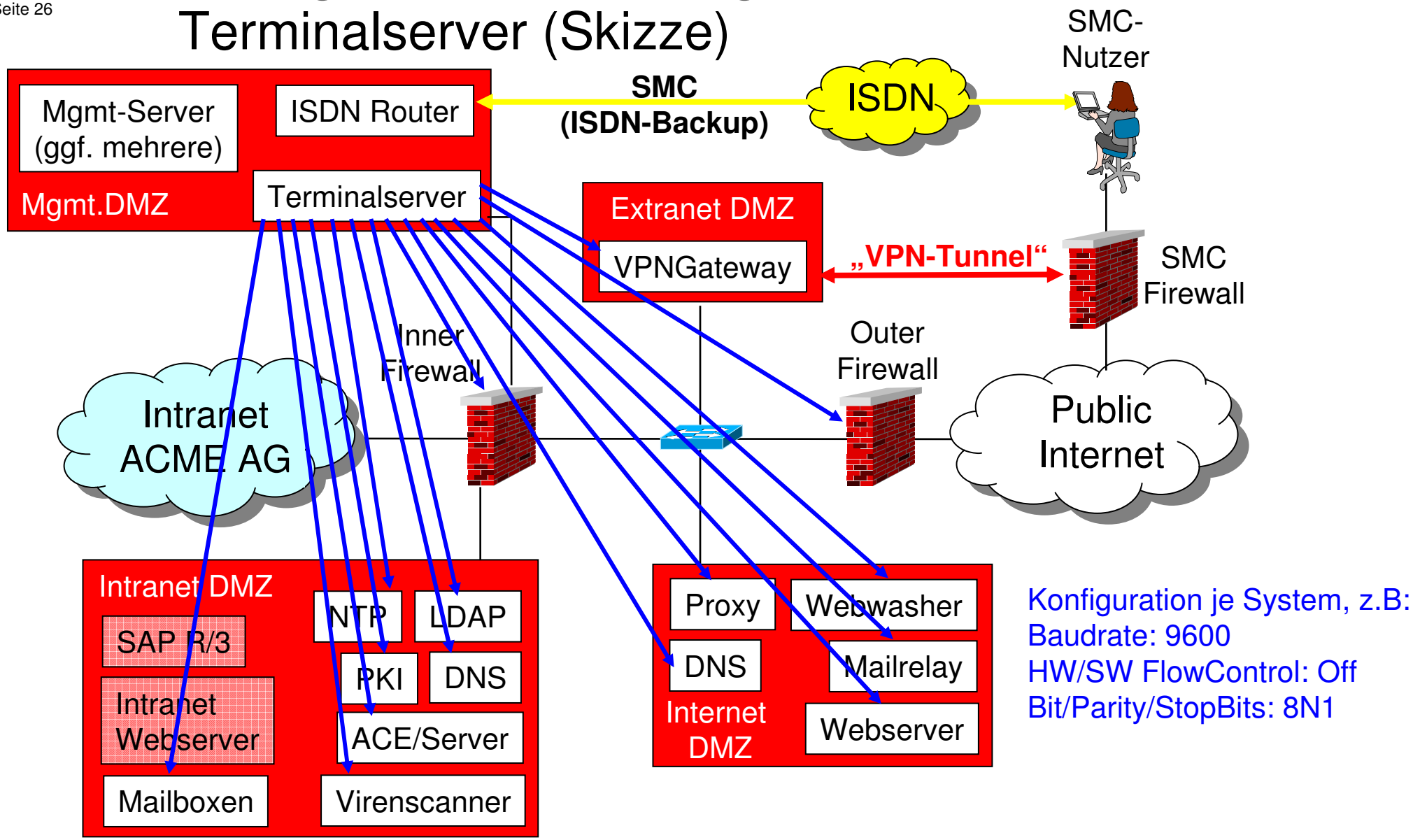


Management der Lösung
Anbindung der Server

- Wirknetz:
  - „Inband-Zugriff“ (Dienstnutzer), Produktivumgebung
- Management-Netz:
  - Ethernet-Schnittstelle (z.B. HP iLO, FSC iRMC)
  - „Outband-Zugriff“ (nur für SMC)
- Backup-Netz:
  - Anschluss von SAN oder NAS
- Serielle Schnittstelle:
  - Anbindung des Servers über einen Terminalserver
  -
- Wirk-, Management und Backup-Netz erfordern zusätzlich:
  - Abschottungsmaßnahmen zur Trennung der Netze
  - Eigene IP-Subnetze, Statische Routen
  - Eigene Layer-2 Infrastruktur (Switches usw.)
  - Zusätzliche Ethernet/Fibre Channel o.ä. Steckkarten auf den Servern



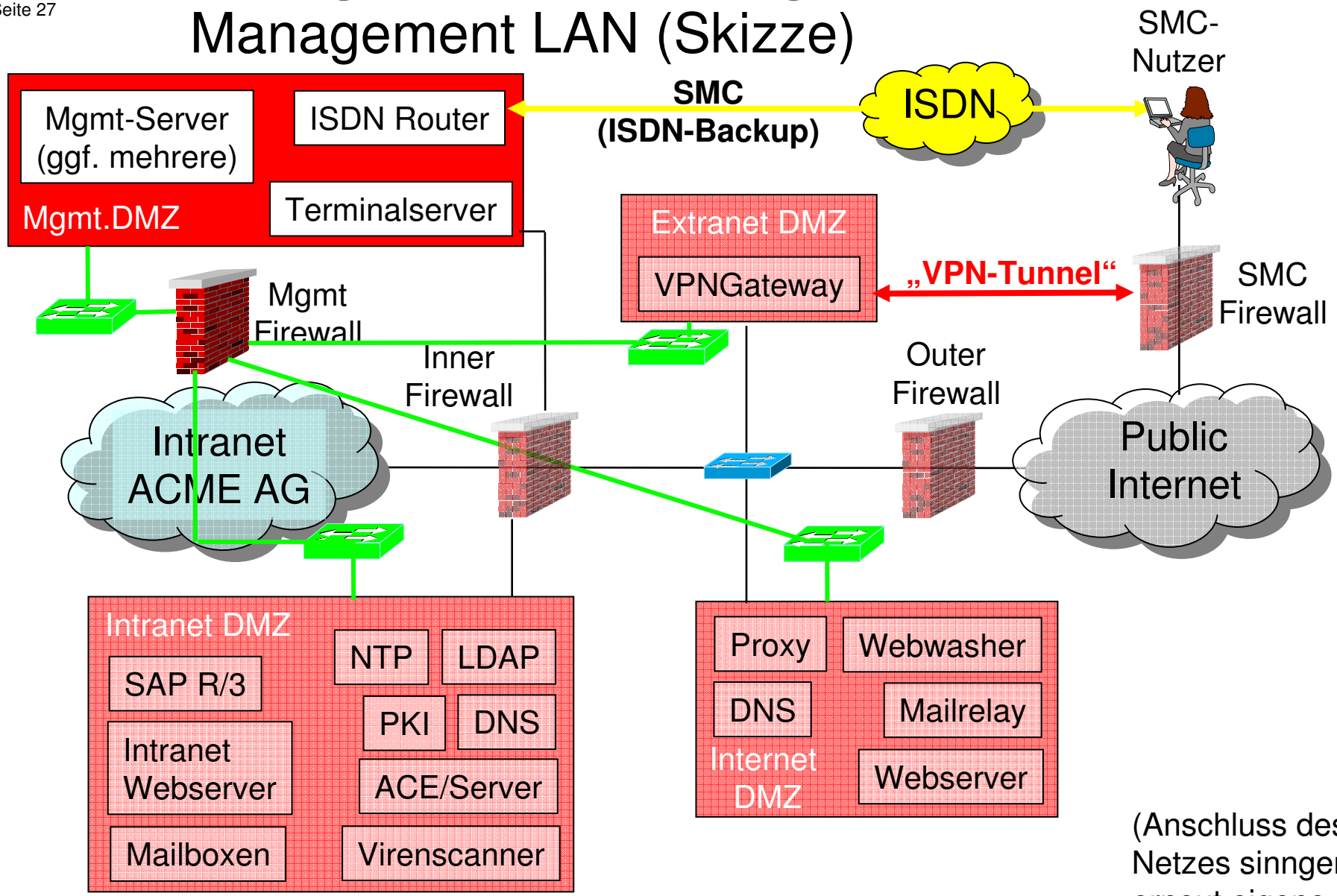
Management der Lösung
Terminalserver (Skizze)



Konfiguration je System, z.B:
Baudrate: 9600
HW/SW FlowControl: Off
Bit/Parity/StopBits: 8N1

Management der Lösung

Management LAN (Skizze)



(Anschluss des Backup-Netzes sinngemäß, d.h. erneut eigene Switches und ggf. noch eine FW!)

Managements der Lösung
Betriebliche Aufgaben (kleine Auswahl)

- Fault/Performance Management:
  - Suchen nach Ursachen von „Problemen aller Art“
  - Backup/Restore von Konfigurationsdateien, Neuinstallation von Servern
  - Überwachung von Servern/Services, z.B. mit SNMP und Nagios
- Change Management:
  - Benutzerverwaltung z.B. Rücksetzen von Passwörtern
  - Bestandsdatenverwaltung (Rack- und Verkabelungsplan, Netz, VLAN- und Routing-Plan, Kommunikationsmatrix, Wartungsinformationen usw.)
- Security Management:
  - Testen und Einspielen von Patches, Bug Fixes usw.
  - Security Audits, Scannen auf offene Ports, Analyse von Logfiles
- Accounting und Reporting:
  - Aufbereitung und Visualisierung von Logdaten o.ä.
  - Erstellen von Statistiken, Trends, Prognosen

Realisierung der Gesamtlösung
Kostenbestandteile – Checkliste

- Corporate Network
  - u.a. Bandbreite, Länge des „Local Loops“, Markt- und Länderspezifika
- Internet-Zugang
  - Anschlussgebühr, Bandbreitenabhängige Grundgebühr und je nach Tarifmodell volumenabhängige Kosten (Euro/Gbyte), ggf. Kosten für Backup
- Housing und zentrale Rechenzentrumsdienste:
  - Benötigte Höheneinheiten (HE) in 19‘‘ Racks, Glasfasern
  - 1 Rack hat ca. 40 HE, wird aber wg. Abwärme nicht voll belegt
  - Backup von Systemen, LAN-Infrastruktur, Zwei Brandabschnitte o.ä.
- Hardware, Software, Lizenzen und Kosten für Wartungsverträge
  - Vor-Ort Replacement Service, Support, Bug-Fixes, Major/Minor Releases usw.
- Kosten für Planung und Realisierung der Lösung (Personentage)
  - Design, Bestellung, Implementierung, Test, Dokumentation, Abnahme, Übergabe
  - Projektmanagement, Steuerung und Koordination von Lieferanten, ...
- Kosten für den Betrieb der Lösung
  - HW (Terminalserver, PowerCycler, Mgmt-Server, Standleitung/ISDN für Mgmt.)
  - Entwicklungs- und Testumgebung (HW und Personentage)
  - Personentage für Fehler-, Change-, Performance-, Security Mgmt., Reporting, ...

Das wärs für heute...

- Literatur: Siehe Linkliste der letzten Vorlesung
- Fragen / Diskussion
- Verbesserungsvorschläge

- Die Folien sind bereits auf die Web-Seite der Vorlesung:
  http://www.nm.ifi.lmu.de

- 19. Juni 2008: WLAN und UMTS
  - Referent: Stefan Emilius, Christian Pauli (beide T-Systems)

- Einen schönen Abend !!!